UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/642,318	08/15/2003	Wade Keith Wan	15065US01	2849

23446 7590 12/24/2008
MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER
SHIFERAW, ELENI A

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
12/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/642,318
Filing Date: August 15, 2003
Appellant(s): WAN ET AL.

Roy B. Rhee
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 09/24/2008 appealing from the Office action mailed 08/25/2008.

1. *Real Party Interest*

A statement identifying the real party in interest is contained in the brief.

2. *Related Appeals and Interferences*

The brief does not contain a statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief. Therefore, it is presumed that there are none. The Board, however, may exercise its discretion to require an explicit statement as to the existence of any related appeals and interferences.

3. *Status of the Claims*

The statement of the status of the claims contained in the brief is correct.

4. *Status of Amendments After Final*

The Appellant's statement of the status of amendments contained in the brief is correct.

5. *Summary of Claimed Subject Matter*

The summary of claimed subject matter contained in the brief is correct.

6. *Ground of Rejection to be Reviewed on Appeal*

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

7. *Claims Appendix*

The copy of the appealed claims contained in the Appendix to the brief is correct.

8. Evidence Relied Upon

US PG Pubs. 20040205095	Gressel et al.	October 14, 2004
USPN 6,993,542	Meiyappan	January 31, 2006
USPN 5,327,522	Furuta	July 5, 1994
US PG Pubs 2003/0072059	Thomas et al.	April 17, 2003
US PG Pubs 2005/0066168	Walmsley	March 24, 2005

9. Ground of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

2. **Claims 1-6, 14-16, and 20-22 are rejected under 35 U.S.C. 102(e) as being anticipated by Gressel et al. 2004/0205095 A1.**

Regarding claim 1, Gressel et al. teaches

- a method of generating pseudo-random numbers using a linear feedback shift register (0044-0046, 0026 and 0098)
- in which the correlation between successive pseudo-random numbers is reduced (0046),

- said method comprising Sampling output sequences of said linear feedback shift register with a specified periodicity (0096, 0046, abstract, 0026-0027, and 0097).

Regarding claim 2, Gressel et al. teaches the method wherein said linear feedback shift register generates said output sequences corresponding to maximal length sequences (0043).

Regarding claim 3, Gressel et al. teaches the method wherein said specified periodicity is equal to the number of bits output by said linear feedback shift register (0175).

Regarding claims 4-6, Gressel et al. teaches the method further comprising periodically switching between iterative outputs generated by two or more linear feedback shift registers (0263-0264, 0281-0282).

Regarding claims 14-16, Gressel et al. teaches the method further comprising operating a nonlinear operator on said pseudo-random number and one or more operands (0217 and 0239).

Regarding claims 20-22, Gressel et al. teaches the method further comprising: receiving said pseudo-random number generated from said linear feedback shift register (0148, 0156; and varying the initial value of said hashing function over time by way of a function operating on one or more variables (0183, 0197, 0372, and 0455).

3. Claims 7-10 and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Furuta et al. 5327522.

Regarding claim 7, Furuta et al. teaches

- a method of generating pseudo-random numbers using linear feedback shift registers (col. 44 lines 55-68)
- in which the correlation between successive pseudo-random numbers is reduced (col. 67 lines 36-col. 68 lines 2),

- said method comprising periodically switching between iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register (col. 67 lines 36-col. 68 lines 2).

Regarding claim 8, Furuta et al. discloses the method wherein said linear feedback shift registers comprise linear shift registers capable of generating maximal length sequences (claim 18).

Regarding claims 9 and 10, Furuta et al. teaches the method wherein said pseudo-random numbers are generated with period equal to the sum of each of the individual linear feedback shift register periods (col. 47 lines 47-col. 48 lines 15).

Regarding claim 19, Furuta et al. teaches the method wherein said one or more variables comprises the configuration of feedback taps associated with said linear feedback shift register (Col. 44 lines 55-col. 45 lines 32).

4. Claims 11-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Thomas et al. 2003/0072059 A1.

Regarding claim 11, Thomas et al. discloses

a method of encrypting a pseudo-random number (claim 3)

generated by a linear feedback shift register (par. 0146 and claim 35)

comprising operating a nonlinear operator on said pseudo-random number and one or more operands (claim 29, and par. 0213, and 0155).

Regarding claim 12, Thomas et al. teaches the method wherein said nonlinear operator comprises an XOR function (0146, 0132).

Regarding claim 13, Thomas et al. teaches the method wherein said one or more operands comprises one operand comprising a unique bit sequence corresponding to the LFSR currently used to generate said pseudo-random number (par. 0125-0127, 0155, 0133, and claim 29).

5. Claim 17 is rejected under 35 U.S.C. 102(e) as being anticipated by Walmsley 20050066168 A1.

Regarding claim 17, Walmsley discloses a method of further encrypting a pseudo-random number (par. 0338, 0344, and 0358) generated from a linear feedback shift register (fig. 9) by using a hashing function (0771, and 0774-0775) comprising:~
receiving said pseudo-random number generated from said linear feedback shift register (0358-0365 and 0942-0934); and varying the initial value of said hashing function over time by way of a function operating on one or more variables (0358-0365 and 0942-0934).

6. Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by Meiyappan USPN 6993542 B1.

Regarding claim 1, Meiyappan discloses a method of generating pseudo-random numbers (col. 1 lines 65-col. 2 lines 2 and col. 1 lines 19-24) using a linear feedback shift register (fig. 1 element 112) in which the correlation between successive pseudo-random numbers is reduced (col. 1 lines 19-24 and abstract), said method comprising sampling output sequences of said linear feedback shift register with a specified periodicity (col. 3 lines 14-32 and fig. 2 element 206).

Claim Rejections - 35 USC § 103

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Furuta et al. 5327522 in view of Gressel et al. 2004/0205095 A1.

Regarding claim 18, Furuta et al. teaches the method further comprising: receiving said pseudo-random number generated from said linear feedback shift register (col. 44 lines 55-68); Furuta et al. fails to varying the initial value of said hashing function over time by way of a function operating on one or more variables.

However Gressel et al. discloses receiving said pseudo-random number generated from said linear feedback shift register (0148, 0156); and varying the initial value of said hashing function over time by way of a function operating on one or more variables (0183, 0197, 0372, and 0455).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings because they are analogous in LFSR random number generation.

One would have been motivated to incorporate the teachings because it would perform verification of initial value.

10. Response to Argument

I. REJECTION OF CLAIMS 1, 3-6, 14-16, AND 20-22 UNDER 35 U.S.C. § 102(e)

A. Independent Claim 1

Regarding argument Gressel failure to disclose “sampling output sequences of linear feedback shift register with a specified periodicity,” appeal brief pages 6-7, argument is not persuasive because Gressel discloses generating *a cyclic output* sequence of pseudorandom binary numbers wherein the cyclic output sequence including a basic sequence which is generated repeatedly, *using clocked* pseudorandom binary number sequence generator (see abstract/par. 0080, and par. 0049).

The examiner interpreted the “specified periodicity” of claim 1 in light of the appellant’s disclosure par. 0024 lines 6-8 wherein “A Linear Feedback Shift Register (LFSR) of any given size n is capable of producing every possible state (outcome) <u>during the period</u> [p=(2^n)-1].” Further, see par 0028 lines 1-4 for specified n bit/digit output (n=3). See par. 0029 lines 3-4 of appellant’s disclosure that discloses “*sampling once every n iterations* prevents revealing …..” The “specified periodicity” of the claim is interpreted as a *period/interval time/clock cycle.* The applied reference Gressel teaches the LFSR register sampling randomly once in 64 system clock cycles see par. 0049. The clocked LFSR of Gressel generates a cyclic output sequence of binary numbers (see 0026-0027 and abstract).

Regarding argument Gressel teaching sampling “after a random waiting interval has elapsed” which is opposite from sampling with a “specified periodicity,” appeal brief page 8, argument is not persuasive because see par. [0047-0049] wherein Gressel discloses *sampling randomly and not more often than once in 64 system clock cycles* (see par. [0047-0049]) and further see par. [0267, and 0175-0177] wherein Gressel discloses a clocked binary random number generator wherein the generator is an electronic oscillator that generates *periodic signal* for synchronization of processes and the randomness of the generator is typically initiated by simultaneously activating a primary clock and a second uncorrelated clock, such that randomizing events occur at intractably difficult to estimate intervals and the pseudorandom modification includes a random slip in which a portion of the cyclic output sequence is omitted (see par. 0088). Therefore Gressel does not teach away from what is recited in claim 1.

B. Dependent claim 3

Regarding argument the applicant could not see how Gressel, at paragraph [0175], shows a teaching of "wherein said specified periodicity is equal to the number of bits output by said linear feedback shift register," appeal brief page 9, argument is not persuasive because Gressel par. [0175] teaches the device (the clocked binary random number generator) generating and outputting random number bits periodically in a time interval and/or Gressel further teaches the clocked pseudorandom binary number sequence generator includes a feedback shift register and wherein the pseudorandom displacement is caused by complementing the serial feedback bit in the feedback shift register using pulsed "1" bits which are externally generated at intractably difficult to estimate intervals of time (see par. [0084]).

C. Dependent claims 4-6

Appellant's argument regarding Gressel failure to teach "periodically switching between iterative outputs generated by two or more linear feedback shift registers," appeal brief pages 10-12, is not persuasive because Gressel on par. [0262-0264] teaches alternating/swapping output between two feedback configurations (see fig. 10) that discloses two nLFSRs 1200 and 1300. Switching/swapping feedback tap configurations (feedback swaps) of the two feedback shift registers 1200 and 1300 are described in (par. [0293]) and further Gressel (par. [0244]) teaches swapping for randomizing the output of LFSR between two sets of feedback taps (configurations) hence, causing alternating generation of *cyclic/periodic* segments from two maximum length linear feedback register sequences. Par. [0281-0282] of Gressel discloses randomizing the three non-linear feedback shift registers nLFSRs 640, 650 and 660 by using slip trigger generator to switch in a regular interval.

D. Dependent claims 14-16

Appellant's argument regarding Gressel failure to teach "operating a nonlinear operator on said pseudo-random number *generated or output by a linear shift register* and one or more operands", appeal brief page 12 last paragraph, is not claimed (the italic part is not claimed). Claim 1 recites generating pseudo-random number by linear feedback shift register and, as cited by the examiner, Gressel par. (0044-0046, 0026 and 0098) discloses a linear feedback shift register generating random numbers.

Appellant's argument regarding Gressel failure to teach "operation performed on the pseudo-random number that is generated *from a shift register*," appeal brief page 12-13 last paragraph, is not persuasive because it is not claimed. Claims 14-16 recite "operating a nonlinear operator on said pseudo-random number and one or more operands." Gressel teaches operating a nonlinear feedback shift register by using a *NAND operator* to insert a zero operand and *NOR operator* to insert a one operand into next output (see par. [0217]). Gressel nLFSR further uses *XOR operator* (see par. [0239]).

Therefore Gressel does not teach away from a "linear feedback shift register."

II. REJECTION OF CLAIM 1 UNDER 35 U.S.C. § 102(e)

A. Independent Claim 1

Appellant's argument regarding Meiyappan failure to disclose "reducing the correlation between successive pseudo-random numbers," Appeal brief pages 15-16, argument is not persuasive because Meiyappan's abstract teaches a generation of truly random numbers using enhanced random number generating technique to achieve unpredictable key security (see also col. 1 lines 19-24). The truly random numbers are generated using the random number generating technique *that includes a method of periodically clocking the output of sampling switch 110* (see col. 3 lines 14-32 and fig. 2 element 206), as the appellant's disclosure discloses, on par. 0028, the use of periodic sampling reduces the correlation between successive outputs of an LFSR, Meiyappan's LFSR 112 also uses periodic sampling and therefore it reduces the correlation between successive outputs of the LFSR.

Regarding argument, according to Meiyappan's fig. 1, the linear feedback shift register is simply input into the sampling switch 110, in which the "sampling switch 110 samples (the N bit sample obtained from the Bit Recorder block 108) during periods when its sampling input line is active and does not sample when its sampling input is inactive," appeal brief pages 17-18, argument is not persuasive because as Meiyappan col. 3 lines 1-32 discloses the *bit recording that is based on random N-bit number generated by the LFSR*, each bit of the N-bit number may be fed to each of N multiplexers, the selected signal for the multiplexers is derived from the LFSR output bits such that each multiplexer outputs a different bit of the N-bit sample output. Therefore the sampling switch 110 is sampling the output of the LFSR 112 and further the output of sampling switch 110 *is periodically clocked* see col. 3 lines 29-32. Therefore the N-bit number is generated by the LFSR 112 and outputted to the bit reorder 108 then to the sampling switch as disclosed in col. 3 lines 1-32 or the sampling switch uses N-bit numbers that are directly outputted from LSFR 112, as shown in fig. 1.

III. REJECTION OF CLAIMS 7-10 AND 19 UNDER 35 U.S.C. § 102(e)

A. Independent Claim 7

Regarding argument since Furuta's "arbitrary number of bits" is shifted after connection of the switching circuit 1309 is switch, Furuta does not teach "periodically switching between iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register," appeal brief page 20, argument is not persuasive Furuta col. 67 lines 51-col. 68 lines 2 teaches switching the switching circuit 1309 in response to the control signal after *a predetermined number of bits* are shifted in the LFSR 1302. Furuta further provides an example wherein this predetermined number of bits corresponds to the number of bits which *are shifted in the LFSR 1302 during one period of the random pulses (periodically switching)*. Therefore Furuta discloses periodically switching between iterative outputs since switching done by Furuta's LFSR is done at a predetermined time interval for example one period.

Regarding argument Furuta failure to teach a "first linear feedback shift register" and a "second linear feedback shift register," appeal brief page 20, argument is not persuasive because col. 67 lines 35-col. 68 line 2 discloses the switching circuit 1309 switching between flip flops 1302(1) and 1302(7) of the random number generator 331. Col. 67 line 49-51 of Furuta discloses the connection of the random number generator 331 shown in Fig. 125 being the same as that shown in Fig. 74. Description for Fig. 74 on col. 44 lines 55-col. 45 lines 5 discloses the flip-flops 1302(1) through 1302(7) are LFSR 1302 registers within the LFSR 331. Therefore there are first LFSR (1302(1)), second LFSR (1302(2)) … seven LFSR (1302(7)) that are switched using switching circuit 1309 (see fig. 74 and 125) and Furuta does not teach away from what is recited in claim 7.

B. Dependent Claims 9-10

Regarding argument Furuta's "a logical sum of logical products" obtained by using an OR circuit 52 not teaching a "period equal to the sum of each of the individual linear feedback shift register periods," appeal brief page 22 par. 2, argument is not persuasive because see col. 47 lines 47-59 wherein Furuta teaches the OR circuit 52 that obtains a logical sum of the logical products and outputs equal logical sum. On fig. 79 the signal period sum of logical product input (Yi ∩ Tij) and (Ym ∩ Tmj) for the OR circuit 52 is equal to the signal period logical sum output (logical sum U(Yi ∩ Tij)).

C. Dependent Claim 19

Regarding argument Furuta col. 44 lines 55-col. 45 lines 32 failure to mention the word "variables" as recited in claim 19 wherein "one or more variables comprises the configuration of feedback taps associated with said linear feedback shift register," appeal brief page 24, is not persuasive because Furuta col. 44 lines 55-col. 45 lines 32 teaches LFSR random number generation using neuron unit that receives input signals (see col. 45 lines 16-32). The OR circuit of neuron unit 50, see fig. 20 and col. 47 lines 47-col. 48 lines 38, receives two input signals (Yi ∩ Tij) and (Ym ∩ Tmj) (*feedback taps*) and outputs (logical sum U(Yi ∩ Tij)). Therefore the variables Y, T, i, j, and m comprises the configuration of feedback taps associated with the LFSR 331.

IV. REJECTION OF CLAIMS 11-13 UNDER 35 U.S.C. § 102(e)

A. Independent Claim 11

Regarding argument Thomas failure to teach "comprising operating a non linear operator on said pseudo-random number and one or more operands, appeal brief pages 25-27, argument is not persuasive because Thomas teaches operating a non-linear shift registers (*operators*), to generate a non-linear filtered output, on a random number and one or more operands (*i.e. first and second taps*) (see par. 0155, 0213 and claim 29).

V. REJECTION OF CLAIM 17 UNDER 35 U.S.C. § 102(e)

A. Independent Claim 17

A typo is noted on page 27 of the appeal brief line 19. The appellant is trying to disclose "Regarding independent *Claim 17*, the office action…" instead of "Regarding independent *Claim 11*, the office action…"

Regarding argument Walmsley failure to teach "varying the initial value of said hashing function over time by way of a function operating on one or more variables," appeal brief page 28-29, argument is not persuasive because Walmsley teaches, on par. *0942-0943*, and as the office corrected the typo (*0942-0943 not 0942-0934)* on page 4 line 10 of the office action mailed on 11/26/2007, the checksum register is used to verify that K1 and K2 (*one or more operands*) have not been altered by an attacker and the authentication protocol of Walmsley passes the chosen random number (*i.e. the initial value*) by encrypting both the chosen random number and its digital signature as disclosed on par. [0358-0365] and Walmsley further discloses varying the initial value of the authentication protocol over time since Walmsley uses encrypted *time varying random number* see par. [0360].

Regarding argument the Walmsley failure to disclose anything about "initial value of said hashing function," appeal brief page 30, argument is not persuasive because the protocol as disclosed on par. [0358-0365] applies a hash MMAC-SHA-1 as further described on par. [0353-0357, 0771 and 0784]. The checksum register discloses running hash algorithm (SHA-1) on the keys and comparing the result against an internal checksum value, (see par. 1330 and page 41 table 17), therefore the checksum register is applying hash function operating on the keys.

Regarding argument "initial value of said hashing function" used to "further encrypt a pseudo-random number generated from a linear feed back shift register," appeal brief page 30, argument is not persuasive because it is not claimed. *Using* the initial value of said hashing function to further encrypt … is not claimed. The claim *preamble* recites "A method of further encrypting a pseudo-random number generated from a linear feedback shift register by using a hashing function comprising:" and the preamble is taught by Walmsley (on par. [0338, 0344, and 0358]) the random number is encrypted see par. [0771, and 0774-0775] with a hash function.

VI. REJECTION OF CLAIM 18 UNDER 35 U.S.C. § 103(a)

A. Dependent Claim 18

Regarding argument Gressel failure to disclose "varying the initial value of said hashing function over time by way of a function operating on one or more variables," appeal brief page 31, argument is not persuasive because Gressel par. 0197 discloses using SHA-1 hash function operating on B and N variables and varying the initial value of said hashing function over time by way of a function operating on one or more variables is disclosed in par. [0455] wherein fig. 33 discloses a random number generating device including device of fig. 10, that is a clocked pseudo-random binary number sequence generator, and a secure Hash Standard Coprocessor, that receive the initial output values from the two nLFSRs operative to compress the data into 160 bit ransom strings. The LSFR of fig. 10 as described on par. [0080] is operative to generate a cyclic output sequence of binary number including a string of binary symbols, the cyclic output sequence including a basic sequence which is generated repeatedly, at least one bit stream generator generating a clocked bit stream including a stream of binary symbols of a first type occasionally interrupted by a binary symbol of a second type, wherein a first varying time interval between the occasional interruptions is intractably correlated to the output sequence of the number sequence generator.

11. *Related Proceeding(s)*

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of the examiner's answer.

12. *Conclusion*

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

December 18, 2008

Conferees:

Nasser Moazami
/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

KimYen Vu

/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435

/Eleni A Shiferaw/
Examiner, Art Unit 2436